

UNITED STATES DISTRICT COURT

for the
Western District of Oklahoma

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

an Apple iPhone, serial number 356857114232013
currently located in secure storage at the Federal
Bureau of Investigation, Oklahoma City

Case No. M-23- **490** -SM

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Western District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
21 U.S.C. § 846
18 U.S.C. § 1956(h)

Offense Description
Drug Conspiracy
Money Laundering Conspiracy

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



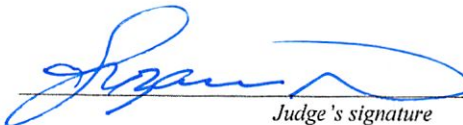
Applicant's signature

Dion Porter, Task Force Officer, (FBI)

Printed name and title

Sworn to before me and signed in my presence.

Date:

6/29/23City and state: Oklahoma City, Oklahoma


Judge's signature

SUZANNE MITCHELL, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of:
(1) a Cricket Wireless cell phone,
IMEI 355171432610087; (2) an
Apple iPhone, serial number
356857114232013; and (3) a
purple Motorola cell phone,
serial number RX-S96767-
MAIN0V01; Currently Stored at
Federal Bureau of
Investigations, Oklahoma City,
Oklahoma**

Case No. M-23-490-SM

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Edward Dion Porter, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—a list of electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request

such a warrant. I am a Task Force Officer (TFO) with the Federal Bureau of Investigations (FBI) assigned to the Oklahoma City office. I have been so assigned since July 2021. As part of my duties as an FBI TFO, I investigate criminal violations relating to drug trafficking and associated money laundering. Prior to being assigned to the FBI, I worked for the Oklahoma City Police Department (OCPD) as a law enforcement officer since 2002. I have received all the required training to work as both a detective with OCPD and a TFO with FBI. This training includes training on drug trafficking and money laundering. I have extensive experience investigating drug trafficking and money laundering related cases.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, and conversations with others who have personal knowledge of the events and circumstances described herein. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18

U.S.C. § 1956(h) (money laundering conspiracy) and 21 U.S.C. § 846 (drug conspiracy) exists and is recorded on the devices described in Attachment A and will be located in the electronically stored information described in Attachment B.

5. “[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.” 18 U.S.C. § 3103a. Venue is proper because the events described in this affidavit took place within the Western District of Oklahoma.

Identification of the Devices to be Examined

6. The property to be searched is a **(1) a Cricket Wireless cell phone, IMEI 355171432610087; (2) an Apple iPhone, serial number 356857114232013; and (3) a purple Motorola cell phone, serial number RX-S96767-MAIN0V01**, (the “Devices”). The Devices are currently located at FBI Oklahoma City located at 3301 W. Memorial Road, Oklahoma City, Oklahoma.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

Probable Cause

8. Since April of 2022, OCPD and FBI have conducted a joint investigation into a Mexico-based drug cartel currently operating within the

Western District of Oklahoma ("DTO"). The DTO utilizes a network of operatives within the United States, including Gerardo Santillan ("Santillan") to collect and launder drug proceeds.

9. In November 2022, FBI developed a cooperating defendant ("CD1").¹ At the time of his/her arrest, CD1 worked as a drug and money courier for the DTO in Oklahoma City. After his/her arrest, CD1 agreed to cooperate with law enforcement and participated in a rule 11 meeting with investigators. During that meeting, CD1 described how he/she received directions via cell phone from his/her boss in the DTO who operated from Mexico. CD1 was shown a photograph of Santillan and identified Santillan as a person (whose name he/she did not know) who CD1 dropped off \$5,000 in drug proceeds to at the direction of his/her Mexico-based boss. CD1 also stated that he/she once lived at a residence in Oklahoma City while working for the DTO that CD1 believed was provided by Santillan.

10. In December 2022, FBI developed a second cooperating defendant ("CD2"). At the time of his/her arrest, CD2 was a drug and money courier operating in Oklahoma City at the direction of the DTO. During a meeting with law enforcement, CD2 was shown a photograph of SANTILLAN and

¹ Like each of the cooperating defendants discussed herein, CD1 was charged in a drug related case. Each of the cooperating defendants discussed herein provided information to law enforcement in hopes of receiving consideration for his/her ultimate sentence.

identified Santillan as the person who CD2 delivered drug proceeds to. CD2 stated that Santillan goes by "Papeles" and that CD2 delivered proceeds to Santillan on three occasions. In total, CD2 estimated that he/she delivered \$26,500 to Santillan.

11. Within weeks of meeting with CD1, law enforcement developed a third cooperating defendant ("CD3"). At the time of his/her arrest, CD3 worked for the DTO as a drug and money courier in Oklahoma City. In a meeting with law enforcement, CD3 described receiving orders from a DTO operative who he/she knew as "Pariente." CD3 said that Pariente gave him/her orders from Mexico via cell phone and provided phone numbers that Pariente used to contact him/her. CD3 went on to state that Pariente directed her to drop off drug proceeds to a man approximately six times. He/she also described several vehicles that he/she knew that man to drive. Law enforcement then showed CD3 photographs of Santillan and two vehicles it knew Santillan to utilize. CD3 positively identified all three photographs and confirmed that Santillan was the man he/she was directed to drop off drug proceeds to. CD3 estimated that he/she dropped off over \$50,000 to Santillan over time.

12. In February 2023, FBI developed a fourth cooperating defendant ("CD4"). At the time of CD4's arrest, he/she was transporting a large load of methamphetamine bound for Oklahoma. CD4 agreed to cooperate with law enforcement and detailed his/her work for the DTO in Oklahoma City. Before

his/her arrest, CD4 was surveilled by law enforcement meeting with Santillan in Oklahoma City on January 9, 2023. On this occasion, Agents were conducting physical surveillance on Santillan. Surveillance observed Santillan meet with an unknown subject in a parking lot in Oklahoma City. The unknown subject got into Santillan's vehicle and was in the vehicle for approximately four minutes before exiting and leaving in his/her own vehicle. The subject was later stopped by law enforcement in that same vehicle and was positively identified. A photograph of the meeting was later shown to CD4 and CD4 identified his/herself as the person that met with Santillan. CD4 advised that he/she was there to drop off drug proceeds to Santillan at the direction of his/her boss in Mexico. CD4 advised that Santillan was one of two main people that he/she dropped off drug proceeds to on a regular basis.

13. CD4 later agreed to speak with law enforcement officers from Oklahoma about his/her dealings with Santillan. CD4 said that he/she had given drug proceeds to Santillan on at least ten separate occasions and estimated the money to be more than \$500,000. CD4 said that he/she had given approximately forty thousand dollars to Santillan 10-15 days prior to his/her arrest on/or around the week of February 7, 2023. CD4 described to officers all the vehicles that Santillan owns and drives on a regular basis. CD4 said that shortly after Ovidio Guzman was arrested in Sinaloa, Mexico, that CD4 was tasked by the DTO to "collect" money in Oklahoma of drug debts that

were owed to the DTO, so that the money could be given to Santillan, who would then in turn see to the money getting back to the DTO in Mexico. CD4 was told that this money would be used in the defense of Ovidio Guzman after his arrest. CD4 identified at least one location in Oklahoma City where he met with Santillan that had already been identified by law enforcement as a location that Santillan regularly picked up money from another drug distributor prior to the arrest of CD4.

14. Toll analysis of a cellular phone number used by Santillan confirmed that he was talking during this time to CD4 and to the Mexico-based boss that works for the DTO. Toll analysis showed that Santillan had communicated with CD4 at least 60 times between December 1, 2022, and January 26, 2023.

15. On June 27, 2023, law enforcement executed a search warrant at the premises located at 2709 NW 112th Street, Oklahoma City, Oklahoma, a primary residence of Gerardo Santillan (the "Subject Premises"). That warrant sought evidence and documents relating to violations of state drug trafficking laws. In addition to the search warrant, Santillan was also subject to a federal arrest warrant for engaging in a money laundering conspiracy. During the execution of the search warrant, law enforcement located the Devices inside the Subject Premises. The Motorola and Cricket Wireless cell

phones were located on Santillan's kitchen counter and the iPhone was located on Santillan's bed.

16. I know, based on my training and experience, that drug trafficking organizations routinely utilize cell phones in furtherance of their drug trafficking and money laundering activities. This use of cell phones almost always leaves behind evidence on the phone itself. This evidence includes communications with coconspirators, call records, location information for the user of the phone during the time crimes were committed, and videos/photographs of drugs, drug proceeds, receipts, or other logs. Further, I know that drug traffickers often utilize multiple cell phones and change cell phones to compartmentalize their illicit activities and thwart law enforcement.

17. I believe, based on my training, experience, and knowledge of this case, that the DTO that Santillan works for is particularly dependent on electronic devices, generally cell phones. I have participated in the arrest of over 25 people associated with this DTO and each of them have utilized a cell phone or multiple cell phones to advance their illicit activities. Further, searches of DTO members' cell phones have provided key evidence in law enforcement's investigation of this DTO, including call records, text messages, WhatsApp messages, photographs, videos, and location data.

18. The Devices are currently in storage at FBI's Oklahoma City office located at 3301 W. Memorial Road, Oklahoma City, Oklahoma. In my training

and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of law enforcement.

Technical Terms

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other

information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can

also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal

computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that each of the Devices have capabilities to allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and a PDA. I also know that each of the Devices is capable of connecting to and surfing the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

21. As set forth in **Attachment B**, the warrant I am applying for requests authorization for search and seizure of only those electronic devices which appear to be found in a location or under circumstances indicating they are not used exclusively for family use or use by children who may reside at the Subject Premises and therefore is limited to computers or electronic devices which are likely to contain the evidence sought by this application.

Electronic Storage and Forensic Analysis

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store

electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

24. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Whatsapp" and "GroupMe." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This

data includes contacts used to conduct illegal activities to include drug trafficking and money laundering.

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to communicate about drug trafficking or associated money laundering, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime

of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

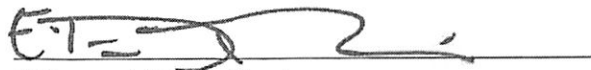
28. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Devices. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law

enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

29. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Edward Dion Porter
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn on this 29th day of June, 2023.



SUZANNE MITCHELL
U.S. Magistrate Judge

ATTACHMENT A

Property to be Searched

The property to be searched is (1) an Apple iPhone, serial number **356857114232013** (the "Device.") The Device is currently located at FBI OKC 3301 W. Memorial Road, Oklahoma City, Oklahoma.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to violations of 18 U.S.C. § 1956(h) (money laundering conspiracy) and 21 U.S.C. § 846 (drug conspiracy) involving Gerardo Santillan, including:

1. Records relating to communication with others as to the criminal offense(s) listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
2. Records relating to documentation or memorialization of the criminal offense(s) listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
3. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into

any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offense(s) listed above;
5. Threatening communications related to the criminal offense(s) listed above;
6. All bank records, checks, credit card bills, account information, and other financial records. Records relating to financial data, to include bank records, checks, credit card bills, account information, and other financial records, electronically stored records showing proof of residence, proof of storage unit use and/or rentals, additional properties owned or documents reflecting stash houses, real estate transaction documents, rental agreements or documents, as well as automotive sale or purchase or financing documents, electronically stored documents purporting to indicate income or salaries received reflecting employment, hours worked, wages earned, withholdings, W-2 and W-4 forms, (blank or executed), state and federal tax returns or documents pertaining to the preparation thereof, electronically stored records showing secret clientele lists, business associates, and diversification of wealth, United States Currency, any other electronically stored tangible items evidencing the obtaining, transfer, secreting, and/or concealment of assets and/or money, electronically stored records, documents, receipts, and/or negotiable instruments which evidence the purchase of negotiable instruments and/or the structuring of currency

transactions to avoid the filing of currency transactions reports and/or the laundering of monetary instruments, electronically stored documents evidencing fruits, instrumentalities, monies, records, and notations, associated with the crime(s) listed above.

7. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
8. All records and information related to the geolocation of the Device(s) and travel in furtherance of the criminal offense(s) listed above; and
9. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.